

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-067477

(43)Date of publication of application : 16.03.2001

(51)Int.Cl. G06T 7/00
G07D 9/00
H04L 9/32

(21)Application number : 11-242168

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 27.08.1999

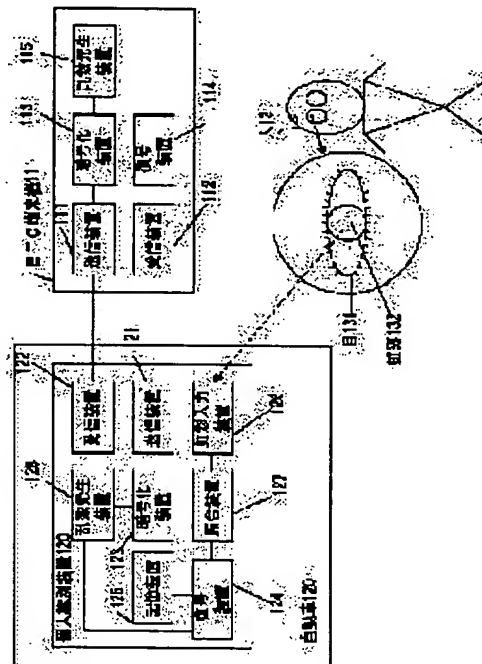
(72)Inventor : SUMI YOSHIKI
KAWASAKI AKIHISA

(54) INDIVIDUAL IDENTIFICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make it difficult to refer to physical feature data of an individual while increasing the security of a terminal device or an individual identifying device of an individual identification system.

SOLUTION: Both an ETC terminal device 11 and an individual identifying device 120 of an automobile 12 are equipped with random number generating devices 115 and 128, ciphering devices 113 and 123, and deciphering devices 114 and 124. The individual identifying device 120 is equipped with an iris input device 126. After mutual authentication is performed between the ETC terminal device 11 and individual identifying device 120 by using random numbers, iris data on a user 13 are inputted and collated with stored ciphered iris data to identify the individual. Consequently, an illegal act by altering the ETC terminal device 11 and individual identifying device 120 is prevented through the mutual authentication and it is made difficult to refer to physical feature data on an individual by ciphering the data to enhance the security of the system.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2001-67477

(P 2001-67477A)

(43) 公開日 平成13年3月16日 (2001.3.16)

(51) Int. Cl. 7	識別記号	F I	テ-マコ-ト' (参考)
G 0 6 T 7/00		G 0 6 F 15/62	4 6 5 K 3E040
G 0 7 D 9/00	4 6 1	G 0 7 D 9/00	4 6 1 A 5B043
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D 5J104
			6 7 5 A

審査請求 未請求 請求項の数 17

O L

(全 10 頁)

(21) 出願番号 特願平11-242168

(22) 出願日 平成11年8月27日 (1999.8.27)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 角 義明

石川県金沢市彦三町二丁目1番45号 株式

会社松下通信金沢研究所内

(72) 発明者 川崎 晃久

神奈川県横浜市港北区綱島東四丁目3番1号

松下通信工業株式会社内

(74) 代理人 100099254

弁理士 役 昌明 (外3名)

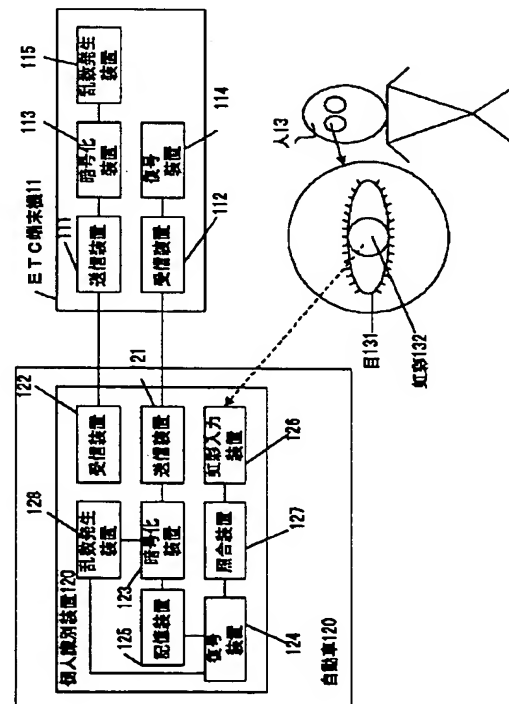
最終頁に続く

(54) 【発明の名称】 個人識別システム

(57) 【要約】

【課題】 個人識別システムの端末機または個人識別装置のセキュリティを高めるとともに、個人の身体的特徴データの参照を困難とする。

【解決手段】 ETC端末機11と自動車12の個人識別装置120の双方に、乱数発生装置115、128と、暗号化装置113、123と復号装置114、124を備える。個人識別装置120に、虹彩入力装置126を設ける。ETC端末機11と個人識別装置120との間で乱数を利用した相互認証の後、利用者13の虹彩データを入力し、記憶してある暗号化虹彩データと照合して個人識別を行う。ETC端末機11及び個人識別装置120の改竄による不正を相互認証で防止するとともに、個人の身体的特徴データを暗号化して参照を困難とし、システムのセキュリティを高める。



【特許請求の範囲】

【請求項 1】 端末機と、個人識別装置と、前記端末機と前記個人識別装置との間で相互認証する手段とを具備する個人識別システムにおいて、前記端末機は、第 1 の送信手段と、第 1 の受信手段と、第 1 の暗号化手段と、第 1 の復号手段とを備え、前記個人識別装置は、第 2 の送信手段と、第 2 の受信手段と、第 2 の暗号化手段と、第 2 の復号手段と、第 1 の記憶手段と、身体的特徴データを入力する第 1 の入力手段と、前記第 1 の記憶手段から取り出して前記第 2 の復号手段で復号したデータと前記身体的特徴データとを照合する照合処理手段とを備えていることを特徴とする個人識別システム。

【請求項 2】 前記端末機と、前記個人識別装置と、前記端末機と前記個人識別装置との間で相互認証する手段とを具備する前記個人識別システムにおいて、前記端末機は、第 2 の記憶手段と、前記第 1 の送信手段と、前記第 1 の受信手段と、前記第 1 の暗号化手段と、前記第 1 の復号手段とを備え、前記個人識別装置は、前記第 2 の送信装置と、前記第 2 の受信手段と、前記第 2 の暗号化手段と、前記第 2 の復号手段と、身体的特徴データを入力する前記第 1 の入力装置と、前記身体的特徴データと前記端末機から受信して前記第 2 の復号手段で復号したデータとを照合する照合処理手段とを備えていることを特徴とする個人識別システム。

【請求項 3】 前記端末機は、暗証番号の前記第 2 の記憶手段を備え、前記個人識別装置は、暗証番号入力手段を備えていることを特徴とする請求項 1、2 記載の個人識別システム。

【請求項 4】 前記端末機は、複数種類の身体的特徴データについて個々に第 2 の入力手段と前記第 2 の記憶手段と照合手段とを備えていることを特徴とする請求項 1、2 記載の個人識別システム。

【請求項 5】 前記端末機及び前記個人識別装置の前記第 1 及び前記第 2 の送信手段並びに受信手段が、それぞれ無線送信手段及び無線受信手段であることを特徴とする請求項 1～4 記載の個人識別システム。

【請求項 6】 前記端末機が IC カードであることを特徴とする請求項 1～5 記載の個人識別システム。

【請求項 7】 前記端末機がナビゲーション装置であることを特徴とする請求項 1～5 記載の個人識別システム。

【請求項 8】 前記端末機が自動料金収受端末機であることを特徴とする請求項 1～5 記載の個人識別システム。

【請求項 9】 前記端末機が車両であることを特徴とする請求項 1～5 記載の個人識別システム。

【請求項 10】 前記身体的特徴データは虹彩データであることを特徴とする請求項 1～9 記載の個人識別システム。

【請求項 11】 前記身体的特徴データは指紋データで

あることを特徴とする請求項 1～9 記載の個人識別システム。

【請求項 12】 前記身体的特徴データは声紋データであることを特徴とする請求項 1～9 記載の個人識別システム。

【請求項 13】 前記身体的特徴データは、歯形データであることを特徴とする請求項 1～9 記載の個人識別システム。

【請求項 14】 前記身体的特徴データは DNA データであることを特徴とする請求項 1～9 記載の個人識別システム。

【請求項 15】 請求項 1～14 記載の個人識別システムにおける端末機であって、不正防止手段を備えていることを特徴とする端末機。

【請求項 16】 請求項 1～14 記載の個人識別システムにおける個人識別装置であって、不正防止手段を備えていることを特徴とする個人識別装置。

【請求項 17】 請求項 1～14 記載の個人識別システムにおける個人識別装置であって、前記身体的特徴データを前記端末機に記憶させる手段を備えたことを特徴とする個人識別装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、個人識別システムに関し、特に、端末機または個人識別装置に格納されている身体的特徴データと、個人識別装置に入力された身体的特徴データを照合することにより個人の識別を行う個人識別システムに関する。

【0002】

【従来の技術】従来、銀行等の金融機関において自動取引装置を用いて入出金取引を行う場合、取引開始前に個人識別を行っている。即ち、他人の口座等を利用した不正な取引が行われないように、暗証番号を入力して本人かどうかの確認を行う処理が予め実施される。ところが、暗証番号が何らかの原因で他人に知られた場合に、不正な取引が行われるおそれがある。そこで、この種の装置におけるより安全な個人識別の方法が研究されている。この種の個人識別方法としては、指紋、声紋、その他各種の個人の特徴点をとらえる方法が開発されている。その中で、例えば、目の網膜や虹彩の特徴を利用した方法が提案されている（特開平 1-306984 号公報、実開平 1-175362 号公報参照）。

【0003】

【発明が解決しようとする課題】しかし、従来の虹彩データなどの身体的特徴データを利用した個人識別では、身体的特徴データがデータベースとして管理されるため、プライバシーの侵害が発生するという問題がある。また、磁気カードなどにおいて個人識別のための虹彩データを利用する場合には、磁気カード内部のデータの改竄により他人へのなりすましによる不正が行われる可能

性がある。さらに、わずかではあるが、識別対象者を本人と認識できなかったり、識別対象者を他人として認識するなどの誤認識をする可能性がある。

【0004】本発明は、上記従来の問題を解決し、身体的特徴データを利用して個人の識別を行うシステムの端末機と個人識別装置の間での相互認証を可能として、安全かつ確実に個人識別を行うことを目的とする。

【0005】

【課題を解決する手段】上記の課題を解決するために、本発明では、端末機と、個人識別装置と、端末機と個人識別装置との間で相互認証する手段とを具備する個人識別システムの端末機に、第1の送信手段と、第1の受信手段と、第1の暗号化手段と、第1の復号手段とを備え、個人識別装置に、第2の送信手段と、第2の受信手段と、第2の暗号化手段と、第2の復号手段と、第1の記憶手段と、身体的特徴データを入力する第1の入力手段と、第1の記憶手段から取り出して第2の復号手段で復号したデータと身体的特徴データとを照合する照合処理手段とを備えた構成とした。

【0006】このように構成したことにより、身体的特徴データに対するプライバシー侵害及び端末機の改竄によるなりすまし及び盗難による被害を防止することができ、安全かつ確実に個人の識別ができる。

【0007】また、端末機と、個人識別装置と、端末機と個人識別装置との間で相互認証する手段とを具備する個人識別システムの端末機に、第2の記憶手段と、第1の送信手段と、第1の受信手段と、第1の暗号化手段と、第1の復号手段とを備え、個人識別装置に、第2の送信装置と、第2の受信手段と、第2の暗号化手段と、第2の復号手段と、身体的特徴データを入力する第1の入力装置と、身体的特徴データと端末機から受信して第2の復号手段で復号したデータとを照合する照合処理手段とを備えた。

【0008】このように構成したことにより、身体的特徴データに対するプライバシー侵害及び端末機の改竄によるなりすまし及び盗難による被害を防止することができ、かつ、個人識別装置が身体的特徴データを持たなくてよい個人識別システムが得られる。

【0009】

【発明の実施の形態】以下、本発明の実施の形態について、図1～図5を参照しながら詳細に説明する。

【0010】（第1の実施の形態）本発明の第1の実施の形態は、ETC端末機と車両の個人識別装置の間で相互認証し、個人識別装置で入力した虹彩データと、記憶してある暗号化虹彩データを復号した虹彩データとを照合して個人識別する個人識別システムである。

【0011】図1は、本発明の第1の実施の形態における個人識別システムの機能ブロック図である。図1において、ETC端末機11は、暗号化されたデータなどを送信する送信装置111と、暗号化されたデータなどを受信

する受信装置112と、データを暗号化する暗号化装置113と、データを復号する復号装置114と、乱数を発生させる乱数発生装置115で構成されている。自動車12は、個人識別装置120を備え、個人識別装置120は、暗号化されたデータなどを送信する送信装置121と、暗号化されたデータなどを受信する受信装置122と、データを暗号化する暗号化装置123と、暗号化されたデータを復号する復号装置124と、暗号化された虹彩データが記憶される記憶装置125と、虹彩データを入力する入力装置126と、記憶装置125から読み出されて復号装置124により復号された虹彩データと入力した虹彩データを照合する照合装置127から構成されている。

【0012】上記のように構成された本発明の第1の実施の形態における個人識別システムの動作を説明する。図1のETC端末機に電源が入ると、乱数発生装置115が乱数を発生し、暗号化装置113により暗号化され、送信装置111により個人識別装置120に送信される。個人識別装置120の受信装置122で受信した暗号化乱数データを、復号装置124により復号する。復号した乱数と、新たに乱数発生装置128で発生させた乱数を連結し、連結したデータを暗号化装置123により暗号化し、暗号化したデータを送信装置121によりETC端末機に送信する。ETC端末機11は、受信装置112で受信したデータを復号装置114で復号する。復号したデータのうちの乱数発生装置115で発生した乱数に対応するデータと、乱数発生装置115で発生した乱数が一致するか比較し、一致したら個人識別装置120の認証ができたこととする。

【0013】ETC端末機11は、復号した乱数発生装置128で発生させた乱数データにあたる乱数データを暗号化装置113で暗号化し、暗号化したデータを送信装置111で個人識別装置120に送信する。個人識別装置120は、受信した、乱数発生装置128で発生した乱数を暗号化したデータを、復号装置124で復号し、復号したデータと、乱数発生装置128で発生した乱数を比較し、一致したら相互認証ができたこととする。

【0014】相互認証ができれば、入力装置126は、人13の目131にある虹彩132を読み取って入力し、入力した虹彩データを照合装置127に出力する。また、記憶装置125から、予め登録されている暗号化された虹彩データを読み出して、復号装置124で復号後、照合装置127に出力する。照合装置127は、復号装置124から入力されたデータと、入力装置126から入力されたデータを比較し、一致した場合、個人を識別できたと判定し、ETC端末機11を使用可能とする。

【0015】なお、相互認証の方式、暗号アルゴリズム、鍵の使用法、鍵の受け渡し方法については、上記の例以外のものでもよい。また、本実施の形態では、身体的特徴データとして虹彩データを例としたが、指紋や声紋や歯形やDNAなどのその他の身体的特徴データを利用してもよい。

【0016】上記のように、本発明の第1の実施の形態では、個人識別システムを、E T C端末機と車両の個人識別装置の間で相互認証し、個人識別装置で入力した虹彩データと、記憶してある暗号化虹彩データを復号した虹彩データとを照合して個人識別する構成としたので、E T C端末機または個人識別装置の改竄による不正が困難となり、また、暗号化して格納してある虹彩データの参照が困難となり、セキュリティが高くなる。

【0017】(第2の実施の形態) 本発明の第2の実施の形態は、ナビゲーション装置と情報提供システムの個人識別装置の間で相互認証し、ナビゲーション装置で入力した声紋データと、個人識別装置に記憶してある暗号化声紋データを復号した声紋データとを照合して個人識別する個人識別システムである。

【0018】図2は、本発明の第2の実施の形態における個人識別システムの機能ブロック図である。図2において、ナビゲーション装置21は、暗号化されたデータなどを送信する送信装置211と、暗号化されたデータなどを受信する受信装置212と、データを暗号化する暗号化装置213と、データを復号する復号装置214と、乱数を発生させる乱数発生装置215と、声紋を入力する声紋入力装置216で構成される。情報提供システム22は、個人識別装置220を備え、個人識別装置220は、暗号化されたデータなどを送信する送信装置221と、暗号化されたデータなどを受信する受信装置222と、データを暗号化する暗号化装置223と、暗号化されたデータを復号する復号装置224と、暗号化された声紋データが記憶される記憶装置225と、記憶装置225の声紋データとナビゲーション装置からの声紋データを照合する照合装置226から構成されている。

【0019】上記のように構成された本発明の第2の実施の形態における個人識別システムの動作を説明する。図2のナビゲーション装置に電源が入ると、乱数発生装置215が乱数を発生し、暗号化装置213により暗号化され、送信装置211により個人識別装置220に送信される。個人識別装置220の受信装置222で受信した暗号化乱数データを、復号装置224により復号する。復号した乱数と新たに乱数発生装置227で発生させた乱数を連結し、連結したデータを暗号化装置223により暗号化し、送信装置221によりナビゲーション装置に送信する。ナビゲーション装置21は、受信装置212で受信したデータを復号装置214で復号し、復号したデータのうち乱数発生装置215で発生した乱数にあたるデータと、乱数発生装置215で発生した乱数が一致するか比較し、一致したら個人識別装置220の認証ができたこととする。

【0020】ナビゲーション装置21は、乱数発生装置227で発生させた乱数データにあたる復号した乱数データを、暗号化装置213で暗号化し、送信装置211で個人識別装置220に送信する。個人識別装置220は、乱数発生装置227で発生した乱数を暗号化したデータを受信して復号

装置224で復号し、復号したデータと乱数発生装置227で発生した乱数を比較し、一致したら相互認証できたこととする。

【0021】相互認証ができれば、ナビゲーション装置21の声紋入力装置216は、人23の発生した声を入力して声紋データを抽出し、暗号化装置213により暗号化し、送信装置211で個人識別装置220に送信する。個人識別装置220は、受信装置222で受信した暗号化された声紋データを復号装置224に出力し、復号装置224は、復号された声紋データを照合装置226に出力する。また、記憶装置225に予め登録されていた声紋データを復号装置224で復号し照合装置226に出力する。照合装置226は、ナビゲーション装置21からの声紋データと記憶装置225からのデータを比較し、一致したら個人を識別できたと判定し、情報提供システム22の情報を利用することを可能とする。情報提供システム22が、音楽データなどをダウンロードできるようなシステムであれば、契約している個人以外はダウンロードできなくなる。

【0022】なお、相互認証の方式、暗号アルゴリズム、鍵の使用法、鍵の受け渡し方法については、上記の例以外のものでもよい。

【0023】上記のように、本発明の第2の実施の形態では、個人識別システムを、ナビゲーション装置と情報提供システムの個人識別装置の間で相互認証し、ナビゲーション装置で入力した声紋データと、個人識別装置に記憶してある暗号化声紋データを復号した声紋データとを照合して個人識別する構成としたので、ナビゲーション装置または個人識別装置の改竄による不正が困難となり、また、暗号化して格納してある声紋データの参照が困難となり、セキュリティが高くなる。

【0024】(第3の実施の形態) 本発明の第3の実施の形態は、I Cカードと自動取引装置の個人識別装置の間で相互認証し、個人識別装置で入力した虹彩データと暗証番号と、記憶してある暗号化虹彩データを復号した虹彩データと暗証番号を照合して個人識別し、不正の場合は警報を発する個人識別システムである。

【0025】図3は、本発明の第3の実施の形態における個人識別システムの機能ブロック図である。図3において、I Cカード31は、暗号化されたデータなどを送信する送信装置311と、暗号化されたデータなどを受信する受信装置312と、データを暗号化する暗号化装置313と、データを復号する復号装置314と、認証などで使用する乱数を発生する乱数発生装置315と、暗証番号や虹彩データなどを記憶する記憶装置316から構成されている。自動取引装置32は、個人識別装置320を備え、個人識別装置320は、暗号化されたデータなどを送信する送信装置321と、暗号化されたデータなどを受信する受信装置322と、データを暗号化する暗号化装置323と、暗号化されたデータを復号する復号装置324と、虹彩データを入力する入力装置325と、虹彩データ及び暗証番号を

照合する照合装置326と、暗証番号を入力する暗証番号入力装置327と、認証などで使用する乱数を発生する乱数発生装置328と、照合装置326により不正と判断された場合に警報を鳴らす不正防止装置329で構成されている。

【0026】上記のように構成された本発明の第3の実施の形態における個人識別システムの動作を説明する。図3のICカード31を情報提供システム22に接続すると、乱数発生装置315が乱数を発生し、暗号化装置313により暗号化され、送信装置311により個人識別装置320に送信される。個人識別装置320の受信装置322で受信した暗号化乱数データを復号装置324により復号する。復号した乱数と新たに乱数発生装置328で発生させた乱数を連結し、連結したデータを暗号化装置323により暗号化し、送信装置321によりICカード31に送信する。ICカード31は、受信装置312で受信したデータを復号装置314で復号し、復号したデータのうち乱数発生装置315で発生した乱数にあたるデータと乱数発生装置315で発生した乱数が一致するか比較し、一致したら個人識別装置320の認証ができたこととする。

【0027】ICカード31は、復号したデータのうち乱数発生装置328で発生させた乱数データにあたる乱数データを暗号化装置313で暗号化し、送信装置311で個人識別装置320に送信する。個人識別装置320は、乱数発生装置328で発生した乱数を暗号化したデータを受信して復号装置324で復号し、復号したデータと乱数発生装置328で発生した乱数を比較し、一致したら相互認証できたこととする。

【0028】相互認証ができれば、入力装置326は、人33の目331にある虹彩332を読み取って入力し、入力した虹彩データを照合装置326に出力する。また、暗証番号入力装置327に暗証番号が入力されると、暗証番号を照合装置326に出力する。また、ICカード31は、相互認証ができれば、記憶装置316に予め登録されている暗証番号及び虹彩データを暗号化装置313で暗号化し、送信装置311により個人識別装置320に送信する。個人識別装置320の受信装置322は、受信した暗号化されたデータを復号装置324で復号し、復号したデータを照合装置326に出力する。照合装置326は、ICカード31から受信した虹彩データ及び暗証番号と、入力装置325から入力された虹彩データ及び暗証番号入力装置327から入力された暗証番号を照合し、虹彩データ及び暗証番号が共に照合できた場合に個人識別できたと判断し、自動取引を開始する。

【0029】照合装置326において不正と判断された場合には、不正防止装置329により警報を鳴らすことができる。また、暗証番号の照合を確認後、入力装置325の入力動作を行うことにより、暗証番号不一致の場合の消費電力を低減することができる。

【0030】なお、以上の説明では、照合装置が個人識

別装置にある場合を説明したが、個人識別装置からの虹彩データ及び暗証番号を送信し、ICカード内に照合装置を備えて照合を行い、照合結果を個人識別装置に送信する場合においても同様の効果が得られる。また、相互認証の方式、暗号アルゴリズム、鍵の使用法、鍵の受け渡し方法については、上記の例以外のものでもよい。

【0031】上記のように、本発明の第3の実施の形態では、個人識別システムを、ICカードと自動取引装置の個人識別装置の間で相互認証し、個人識別装置で入力した虹彩データと暗証番号と、記憶してある暗号化虹彩データを復号した虹彩データと暗証番号を照合して個人識別し、不正の場合は警報を発する構成としたので、ICカードまたは個人識別装置の改竄による不正が困難となり、また、暗号化して格納してある虹彩データの参照が困難とない、セキュリティが高くなる。

【0032】（第4の実施の形態）本発明の第4の実施の形態は、非接触ICカードとホームセキュリティシステムの個人識別装置の間で相互認証し、個人識別装置で入力した虹彩データおよび声紋データと、記憶してある暗号化虹彩データおよび声紋データを復号したデータを照合して個人識別する個人識別システムである。

【0033】図4は、本発明の第4の実施の形態における個人識別システムの機能ブロック図である。図4において、非接触ICカード41は、暗号化されたデータなどを送信する送信装置411と、暗号化されたデータなどを受信する受信装置412と、データを暗号化する暗号化装置413と、データを復号する復号装置414と、認証などで使用する乱数を発生する乱数発生装置415と、暗証番号や虹彩データなどを記憶する記憶装置416から構成される。ホームセキュリティシステム42は、個人識別装置420を備え、個人識別装置420は、暗号化されたデータなどを送信する送信装置421と、暗号化されたデータなどを受信する受信装置422と、データを暗号化する暗号化装置423と、暗号化されたデータを復号する復号装置424と、虹彩データを入力する虹彩入力装置425と、虹彩データ及び暗証番号を照合する照合装置426と、声紋データを入力する声紋入力装置427と、認証などで使用する乱数を発生する乱数発生装置428と、照合装置426の個人識別の結果により動作する電子錠429で構成されている。

【0034】上記のように構成された本発明の第4の実施の形態における個人識別システムの動作を説明する。図4の非接触ICカード41をホームセキュリティシステム42に接続すると、乱数発生装置415が乱数を発生し、暗号化装置413により暗号化され、送信装置411により個人識別装置420に送信される。個人識別装置420の受信装置422で受信した暗号化乱数データを復号装置424により復号する。復号した乱数と新たに乱数発生装置428で発生させた乱数を連結し、連結したデータを暗号化装置423により暗号化し、送信装置421により非接触ICカード

41に送信する。非接触 IC カード 41 は、受信装置 412 で受信したデータを復号装置 414 で復号し、復号したデータのうち乱数発生装置 415 で発生した乱数にあたるデータと、乱数発生装置 415 で発生した乱数が一致するか比較し、一致したら個人識別装置 420 の認証ができたこととする。

【0035】非接触 IC カード 41 は、復号したデータのうち乱数発生装置 428 で発生させた乱数データにあたる乱数データを暗号化装置 413 で暗号化し、送信装置 411 で個人識別装置 420 に送信する。個人識別装置 420 は、乱数発生装置 428 で発生した乱数を暗号化したデータを受信して復号装置 424 で復号し、復号したデータと、乱数発生装置 428 で発生した乱数を比較し、一致したら相互認証できたこととする。

【0036】相互認証ができれば、入力装置 426 は、人 43 の目 431 にある虹彩 432 を読み取って入力し、入力した虹彩データを照合装置 426 に出力する。また、人 43 が、自分自身の名前を発声することにより得られる声紋データ 433 を声紋入力装置 427 から入力し、照合装置 426 に出力する。また、非接触 IC カード 41 は、相互認証ができれば、記憶装置 416 に予め登録されている虹彩データ及び声紋データを暗号化装置 413 で暗号化し、暗号化したデータを送信装置 411 により個人識別装置 420 に送信する。個人識別装置 420 の受信装置 422 は、受信した暗号化されたデータを復号装置 424 で復号し、照合装置 426 に出力する。照合装置 426 は、非接触 IC カード 41 から受信した虹彩データ及び声紋データと、虹彩入力装置 425 及び声紋入力装置 427 から入力された虹彩データ及び声紋データを照合し、虹彩データ及び声紋データが共に照合できた場合に個人識別できたと判断する。個人識別ができた場合には、電子錠 429 をアンロックする。個人識別ができない場合は、電子錠 429 をロック状態のままとする。また、虹彩データの照合または声紋データの照合のいずれか一方の照合を確認後、もう一方の照合を開始することにより、照合不一致の場合の消費電力を低減することができる。

【0037】なお、以上の説明では、照合装置が個人識別装置にある場合を説明したが、個人識別装置から虹彩データ及び声紋データを非接触 IC カードに送信し、非接触 IC カード内に照合装置を備えて照合を行い、照合結果を個人識別装置に送信する場合においても同様の効果が得られる。また、相互認証の方式、暗号アルゴリズム、鍵の使用法、鍵の受け渡し方法については、上記の例以外のものでもよい。また、本実施の形態では、虹彩データおよび声紋データの照合結果の論理積を判定結果としたが、複数の身体的特徴データの照合結果をどのようにしてシステムとしての照合結果とするかは、目的に応じて適宜決定すればよい。

【0038】上記のように、本発明の第 4 の実施の形態では、個人識別システムを、非接触 IC カードとホーム

セキュリティシステムの個人識別装置の間で相互認証し、個人識別装置で入力した虹彩データおよび声紋データと、記憶してある暗号化虹彩データおよび声紋データを復号したデータを照合して個人識別する構成としたので、非接触 IC カードまたは個人識別装置の改竄による不正が困難となり、また、暗号化して格納してある虹彩データおよび声紋データの参照が困難となり、セキュリティが高くなる。

【0039】（第 5 の実施の形態）本発明の第 5 の実施の形態は、車両と車両管理システムの個人識別装置の間で相互認証し、車両で入力した虹彩データおよび指紋データと、記憶してある暗号化虹彩データおよび指紋データを復号したデータを照合して個人識別する個人識別システムである。

【0040】図 5 は、本発明の第 5 の実施の形態における個人識別システムの機能ブロック図である。図 5 において、車両 51 は、暗号化されたデータなどを送信する送信装置 511 と、暗号化されたデータなどを受信する受信装置 512 と、データを暗号化する暗号化装置 513 と、データを復号する復号装置 514 と、認証などで使用する乱数を発生させる乱数発生装置 515 と、虹彩データを入力する虹彩入力装置 516 と、指紋データを入力する指紋入力装置 517 から構成されている。車両管理システム 52 は、個人識別装置 520 を備え、個人識別装置 520 は、暗号化されたデータなどを送信する送信装置 521 と、暗号化されたデータなどを受信する受信装置 522 と、データを暗号化する暗号化装置 523 と、暗号化されたデータを復号する復号装置 524 と、暗号化した虹彩データ及び指紋データを記憶する記憶装置 527 と、虹彩データ及び指紋データを照合する照合装置 526 と、認証などで使用する乱数を発生させる乱数発生装置 525 と、照合装置 526 により個人識別の結果により動作する車両制御装置 528 で構成されている。

【0041】上記のように構成された本発明の第 5 の実施の形態における個人識別システムの動作を説明する。図 5 の車両 51 のシートに座ると、乱数発生装置 515 が乱数を発生し、暗号化装置 513 により暗号化され、送信装置 511 により個人識別装置 520 に送信される。個人識別装置 520 の受信装置 522 で受信した暗号化乱数データを、復号装置 524 により復号する。復号した乱数と新たに乱数発生装置 525 で発生させた乱数を連結し、連結したデータを暗号化装置 523 により暗号化し、送信装置 521 により車両 51 に送信する。車両 51 は、受信装置 512 で受信したデータを復号装置 514 で復号し、復号したデータのうち乱数発生装置 515 で発生した乱数にあたるデータと、乱数発生装置 515 で発生した乱数が一致するか比較し、一致したら個人識別装置 520 の認証ができたこととする。

【0042】車両 51 は、復号したデータのうち乱数発生装置 528 で発生させた乱数データにあたる乱数データを暗号化装置 513 で暗号化し、送信装置 511 で個人識別装置

520に送信する。個人識別装置520は、乱数発生装置528で発生した乱数を暗号化したデータを受信して復号装置524で復号し、復号したデータと乱数発生装置528で発生した乱数を比較し、一致したら相互認証できたこととする。

【0043】相互認証ができれば、虹彩入力装置516は、人53の目531にある虹彩532を読み取って入力し、入力した虹彩データを暗号化装置513により暗号化し、送信装置511で個人識別装置520に送信する。また、指紋入力装置は人53の指紋533を入力し、暗号化装置513により暗号化し、送信装置511で個人識別装置520に送信する。個人識別装置520の受信装置522は、暗号化された虹彩データ及び指紋データを受信すると、復号装置524により復号して照合装置526に出力する。また、車両管理システム51は、相互認証ができれば、記憶装置527に予め登録されている虹彩データ及び指紋データを復号装置524で復号し、照合装置526に出力する。照合装置526は、車両51から受信した虹彩データ及び指紋データと記憶装置527から読み出した虹彩データ及び指紋データを照合し、照合結果を車両制御装置528に送信する。

【0044】照合の結果、個人識別ができていれば、車両51のエンジンを起動するよう車両51に指示する。照合結果において個人識別できず、不正と判定された場合には車両51のエンジンは起動できない。また、個人識別できた場合においても、個人の運転歴や技量などに応じて、速度制限などを車両51に送信して、交通事故を削減することができる。また、虹彩データの照合または指紋データの照合のいずれか一方の照合を確認後、もう一方の照合を開始することにより、照合不一致の場合の消費電力を低減することができる。

【0045】なお、以上の説明では、照合装置が個人識別装置にある場合を説明したが、個人識別装置から虹彩データ及び指紋データを車両に送信し、車両に照合装置を備えて照合を行い、照合結果を個人識別装置に送信する場合においても同様の効果が得られる。また、相互認証の方式、暗号アルゴリズム、鍵の使用方法、鍵の受け渡し方法については、上記の例以外のものでもよい。

【0046】上記のように、本発明の第5の実施の形態では、個人識別システムを、車両と車両管理システムの個人識別装置の間で相互認証し、車両で入力した虹彩データおよび指紋データと、記憶してある暗号化虹彩データおよび指紋データを復号したデータを照合して個人識別する構成としたので、車両または個人識別装置の改竄による不正が困難となり、また、暗号化して格納してある虹彩データおよび指紋データの参照が困難となり、セキュリティが高くなる。

【0047】

【発明の効果】上記の説明から明らかなように、本発明

では、端末機と個人識別装置との間で相互認証する手段を備えた個人識別システムの端末機に、第1の送信手段と、第1の受信手段と、第1の暗号化手段と、第1の復号手段とを備え、個人識別装置に、第2の送信手段と、第2の受信手段と、第2の暗号化手段と、第2の復号手段と、第1の記憶手段と、身体的特徴データを入力する第1の入力手段と、第1の記憶手段から取り出して第2の復号手段で復号したデータと身体的特徴データとを照合する照合処理手段とを備えたので、身体的特徴データに対するプライバシー侵害及び端末機の改竄によるなりすまし及び盗難による被害を防止することができ、身体的特徴データを本人以外に安易に管理されることなく、安全かつ確実に個人の識別ができるという効果が得られる。

【図面の簡単な説明】

【図1】第1の実施の形態における個人識別システムの構成図、

【図2】第2の実施の形態における個人識別システムの構成図、

【図3】第3の実施の形態における個人識別システムの構成図、

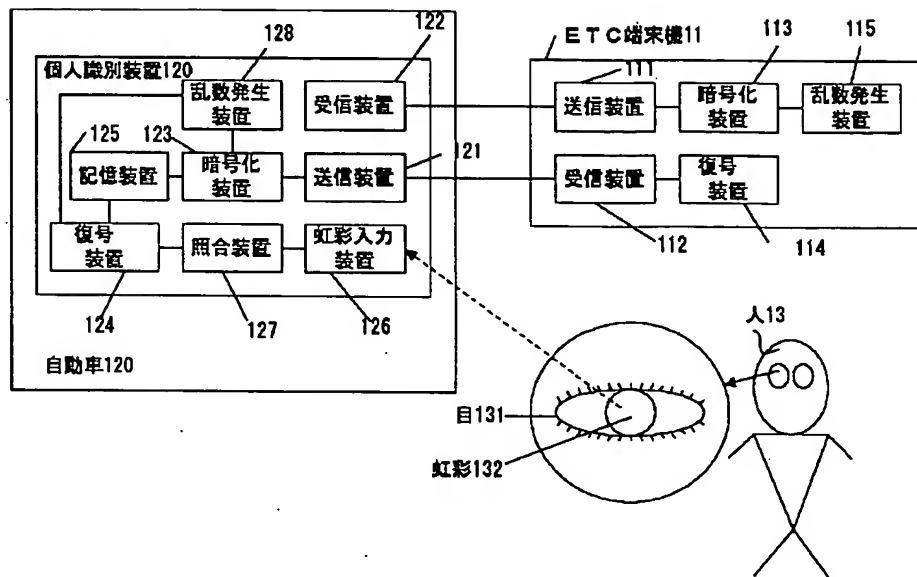
【図4】第4の実施の形態における個人識別システムの構成図、

【図5】第5の実施の形態における個人識別システムの構成図である。

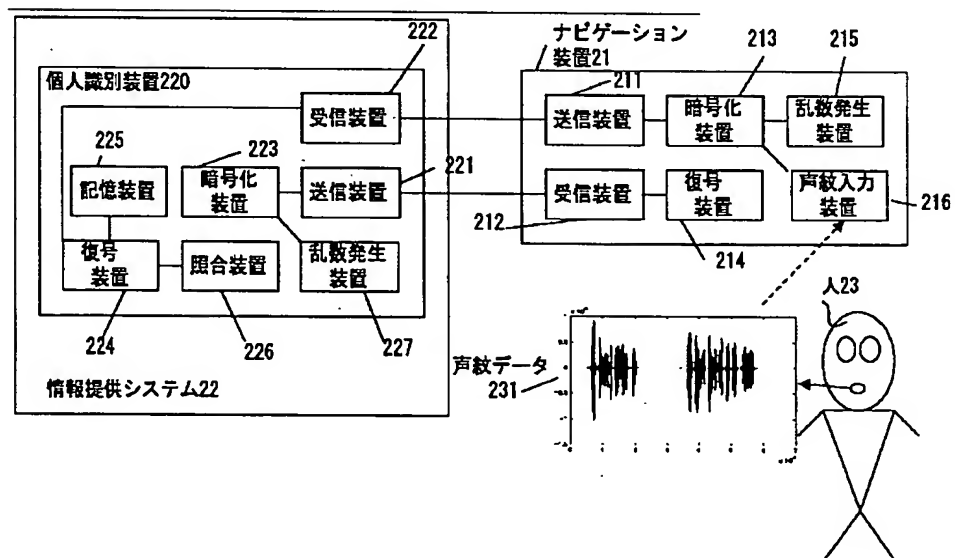
【符号の説明】

111、211、311、411、511	送信装置（端末機側）
112、212、312、412、512	受信装置（端末機側）
113、213、313、413、513	暗号化装置（端末機側）
114、214、314、414、514	復号装置（端末機側）
115、215、315、415、515	乱数発生装置（端末機側）
121、221、321、421、521	送信装置（個人識別装置側）
122、222、322、422、522	受信装置（個人識別装置側）
123、223、323、423、523	暗号化装置（個人識別装置側）
124、224、324、424、524	復号装置（個人識別装置側）
128、227、328、428、525	乱数発生装置（個人識別装置側）
127、226、326、426、526	照合装置
125、225、316、416、527	記憶装置
126、325、425、516	虹彩入力装置
216、427	声紋入力装置
517	指紋入力装置
327	暗証番号入力装置

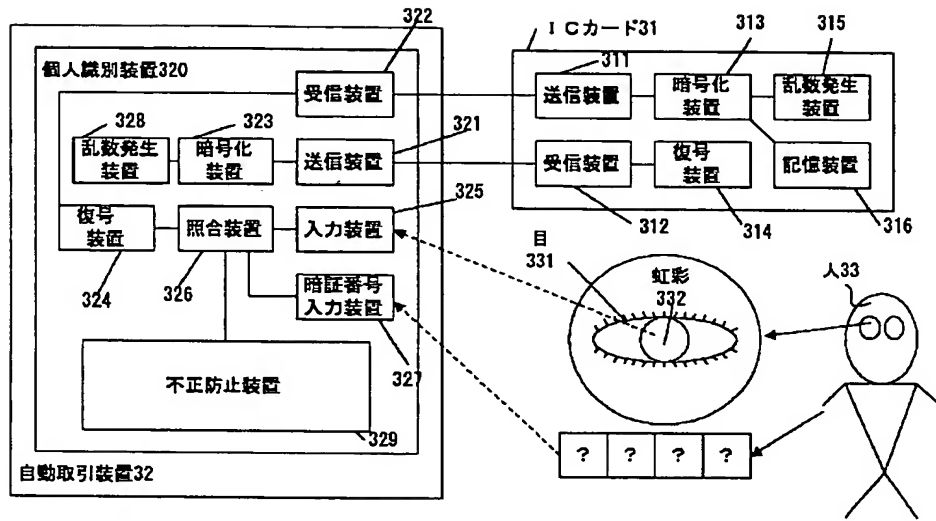
【図1】



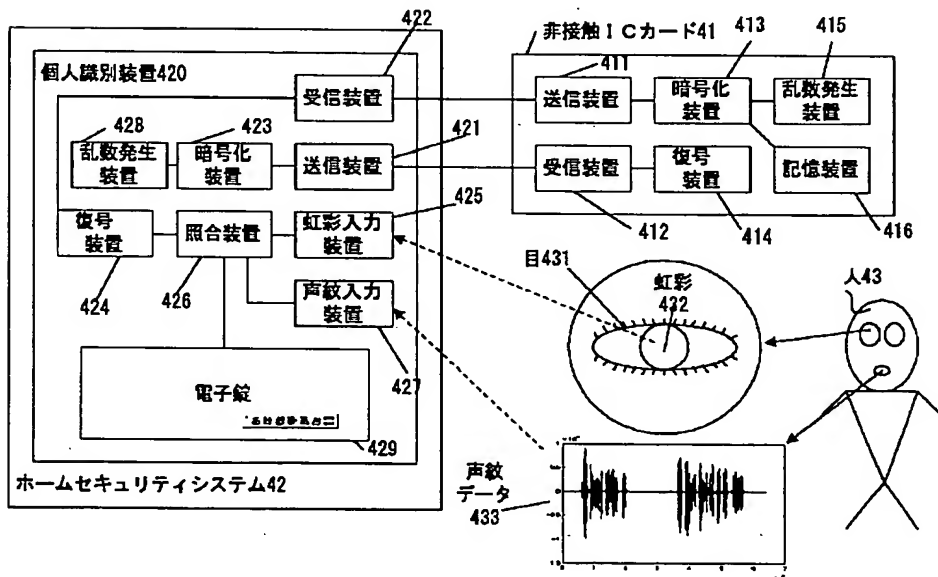
【図2】



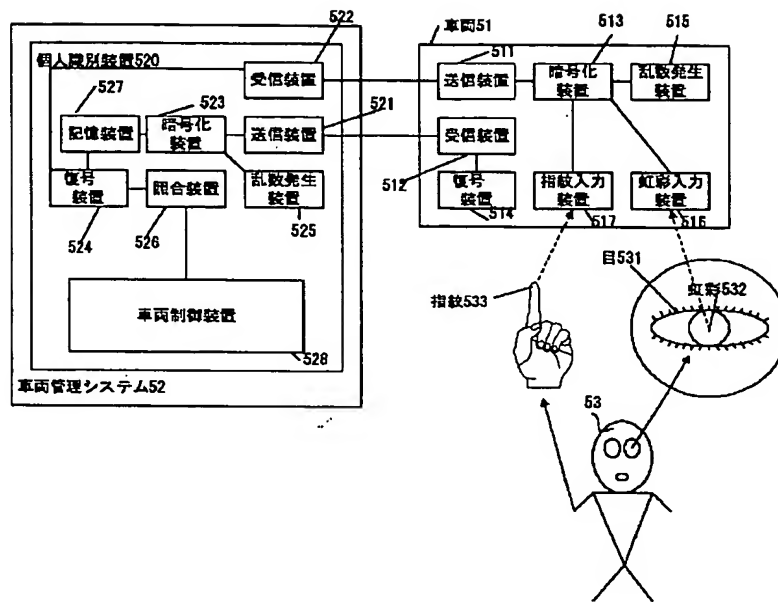
【図3】



【図4】



【図5】



フロントページの続き

Fターム(参考) 3E040 AA03 BA12 CB01 DA02 FH05
 FL04
 5B043 AA01 AA09 BA02 BA04 BA05
 BA07 CA09 FA02
 5J104 AA07 KA01 KA04 KA16 KA17
 KA18 KA19 NA35 NA38 PA00